CROWDSTRIKE

CST 330 – CREATING INTELLIGENCE WITH FALCON

This two-day instructor-led course introduces the doctrinal concepts of gathering and analyzing information to create intelligence products – it includes Cyber Threat Intelligence methodologies but is more broadly focused on general intelligence doctrine. This is an introductory-level intelligence course and is appropriate for techies and non-techies alike who have little or no experience in intelligence functions and production. It includes practical labs for students to develop hands-on skills.

PREREQUISITES

This hands-on course is intended for managers, report writers, intelligence consumers, and analysts of all types – there are no prerequisites. Students who are not familiar with the various CrowdStrike Falcon applications are strongly encouraged to take the included self-paced CrowdStrike Falcon introductory courses on CrowdStrike University – FHT 100: Falcon Platform Overview (11 mins 37 secs) and FHT 101: Falcon Platform Technical Fundamentals (2 hrs 58 mins 48 secs).

To obtain the maximum benefit from this class, you should meet the following requirements:

- Completion of FHT 100 & FHT 101 course material in CrowdStrike University (or experience using CS Falcon)
- Able to understand course curriculum presented in English
- Perform basic operations on a personal computer
- Be familiar with the Microsoft Windows environment

CLASS MATERIAL

Once registered for the course, associated materials may be downloaded from CrowdStrike University.

LEARNING OBJECTIVES

Students who complete this course should be able to:

- Retrieve intelligence reporting and data from various Falcon applications
- Relate basic intelligence processes and concepts to technical data
- Justify proposed security changes to an environment based on own intelligence analysis
- Support your organization's overall security posture by contributing customized, high-level cyber threat reporting

The course includes multiple hands-on labs that allow students to apply what they have learned in the workshop.

REGISTRATION

For a list of scheduled courses and registration access, please log into your CrowdStrike University account.
This course requires four training credits. If you do not have access to CrowdStrike University, need to purchase training credits or need more information, please contact sales@crowdstrike.com.

INTRODUCTION

- **Who we are**
- **Who you are**
- **Admin items**
- **Course Overview/Agenda**

CROWDSTRIKE FALCON

- **Falcon Applications**
- **Falcon Intelligence**
  - Review of each Falcon Intel module
- **Student Exercise**
  - Discover detection in Insight and follow links to associated intel reporting

INTELLIGENCE 101

- **Concepts of Intelligence**
  - Contrasting information from intelligence
  - Intel as a process, product, and organization
  - Intro to tactical, operational, and strategic intelligence
  - Goals of an intelligence program
  - Various types of intelligence
- **Characteristics of Effective Intelligence**
  - Attributes of effective intelligence
  - Intelligence frameworks
  - Creating a flexible framework
  - High-order intel program capabilities
- **The Intelligence Process**
  - The Intelligence Cycle & Process
  - Key considerations of an intel framework
- **Intelligence Consumers**
  - Various levels of consumers
  - Consumer level-appropriate reporting
- **Intelligence Reach**
  - External collaboration
  - Intel sharing platforms
  - CrowdStrike Intelligence

INTEL REQUIREMENTS

- **Requirements process**
- **Framing the intel problem**
- **Intro to Structured Argumentation**
- **Forming a requirement hierarchy**
- **Student Exercise**
  - Group exercise to create standing and ad-hoc requirements

INTEL COLLECTION

- **Selecting Sources of Information**
- **Collection aggregation and storage**
- **Legalities of collection**
- **Timing of collection**
- **Student Exercise**
  - Group exercise to identify and gather sources of information

INTEL COLLECTION

- **Concept of exactness**
- **Types of analysis**
- **The analytic process**
- **Analytic views and models**
- **Traits of a good analyst**
- **Student Exercise**
  - Individual and group tasks to analyze collected information

INTEL PRODUCTION

- **Echelons of reporting**
- **Proper report formatting**
- **The reporting framework**
- **Challenges of production**
- **Student Exercise**
  - Individual and group tasks to report on collected and analyzed information/intelligence

FRAMEWORK VALIDATION

- **Intelligence framework concepts**
- **Intelligence validation**
- **Framework validation**
- **Student Exercise**
  - Group discussion and validation of student-built intel framework

FALCON SPOTLIGHT & FALCON X

- **Introduction to Falcon Spotlight and Falcon X**